**常見的社交工程攻擊方式有哪些?應如何防範?**

資料來源：資通安全處

社交工程 (Social Engineering) 係利用人性弱點，應用簡單的溝通和欺騙技倆，以獲取帳號、通行碼、身分證號碼或其他機敏資料，來突破校園的資通安全防護，遂行其非法的存取、破壞行為。  
  
常見的社交工程攻擊方式如下︰  
●利用電話佯裝資訊人員，騙取帳號及通行碼。  
●偽裝委外廠商之維護人員或上級單位人員，乘機騙取帳號及通行碼。  
●利用電子郵件誘騙使用者登入偽裝之網站以騙取帳號及通行碼，如網路釣魚。  
●利用電子郵件誘騙使用者開啟檔案、圖片，以植入惡意程式、暗中收集機敏性資料。  
●利用提供工具、檔案、圖片為幌子，誘騙使用者下載，如偽裝的修補程式 、 p2p 下載軟體、工具軟體等，乘機植入惡意程式、暗中收集機敏性資料。  
●利用即時通訊軟體如 MSN ，偽裝親友來訊，誘騙點選來訊中之連結後中毒。  
社交工程雖然利用人性弱點來騙取機敏資料，讓人覺得防不勝防，但如果能隨時提高警覺，不未經確認即提供資料、不開啟來路不明的電子郵件及附加檔案、不連結及登入未經確認的網站、不下載非法軟體及檔案，就能避免社交工程的攻擊傷害。